Insights on protecting crypto ops

Why a couple advanced controls isn't enough

Ethan Johnson
Next Encrypt

What is cryptocurrency

Simple definition - a digital or virtual currency secured by cryptography, operating on a decentralized system

Billions worth of crypto are moving every day, protected by cryptography, digital signatures, and broader information security practices

It's also sadly considered:

.. dangerous
.. contributing to the rise of ransomware
.. an avenue for social engineering, scams, theft, and money laundering

I personally hope it plays a major role in the future of finance

Why it's attacked so much

1) Substantial value - market cap in the trillions
2) Ease of theft & reuse
3) Risk and impacts of getting caught

It's often considered easier and safer to threat actors than physical theft and robbery

Risk = function (assets, threats, controls, vulnerabilities)

Assets and potential risks have a strong relationship

What's been going wrong

Scams
Fraud
Social engineering
Stolen keys
Hacked smart contracts
Malicious tokens and smart contracts
Advanced attacks on companies with large funds
Physical attacks and kidnappings
Misunderstandings about keys, wallets, and custody exploited
.. and many more

Recently over $1 Billion was lost in a single incident

What is crypto ops

Unless a system is fully automated end-to-end, it's *operated* by individuals
Think payments, transfers, investing, settling, accounting, etc.

***People** are involved in deciding how funds are stored and transferred
These transactions tend to be handled with **systems and processes**

The technologies, methods, mechanisms, etc. are a bit different from traditional finance, with lots of the same underlying concepts

The types of cryptocurrency organizations, and related ops, can vary widely. E.g.

Exchanges and Trading, Lending, Mining, Stablecoins, Gaming, NFTs,
Wallet Software, Funds Transfer Systems, Payments, Chain Tracing & Analytics,
Monitoring Products, Custody, Web3 Infra providers, Layer 1s, Layer 2s

Zooming in.. the big hack

Everyone's asking about the big newsworthy ~1.5 Billion hack

In the realm of self-custody, a couple key controls have become common, and I'm fairly certain were involved:

1) Multiple signature systems and hardware wallets
2) Transaction checks e.g. simulations, wallet address checks or allow-lists, etc.

With a multisig, a threshold of signers must be reached before transactions can be executed, funds can move, etc.

Some recent hacks likely involving these controls:
~$1.5 Billion Multisig, hardware wallets
~ $58 Million Multisig, hardware wallets
~ 235 Million Multisig, hardware wallets & 3rd party signer

Zooming in.. (continued)

Publicly released details on the ~1.5 Billion hack

The organization providing publicly available multisig capabilities was breached

From what I found in the news:

- A developer's computer was hacked
- Some amount of production access to their AWS S3 was gained
- Malicious javascript ended up in their AWS S3 bucket
    - Designed to activate under certain limited circumstances

* Note - at that point, not much unique to the crypto and web3 world

Sounds a lot like a *watering hole* attack

Zooming in.. (continued)

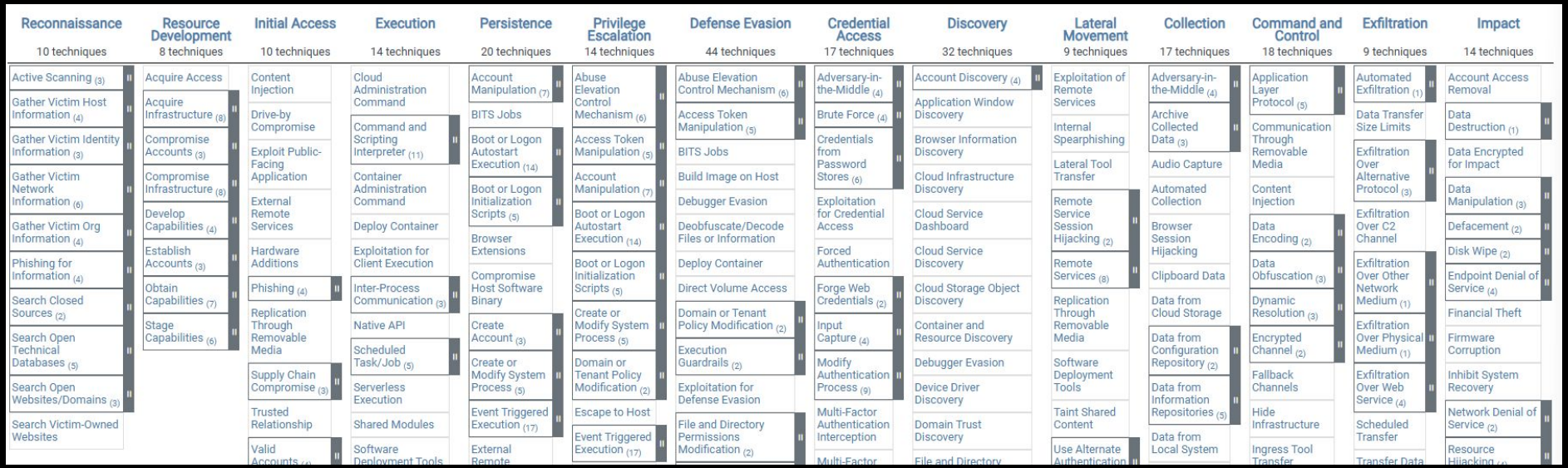
The primary target of the attack was a crypto company with substantial assets

While performing a (likely) routine operation with their multisig wallet, which holds substantial funds

- The malicious javascript seems to have tricked them
- A seemingly routine transfer interacted with a new and unexpected wallet
- Substantial fund loss ensued

From another lens

ATT&CK®



Reconnaissance (10 techniques)	Resource Development (8 techniques)	Initial Access (10 techniques)	Execution (14 techniques)	Persistence (20 techniques)	Privilege Escalation (14 techniques)	Defense Evasion (44 techniques)	Credential Access (17 techniques)	Discovery (32 techniques)	Lateral Movement (9 techniques)	Collection (17 techniques)	Command and Control (18 techniques)	Exfiltration (9 techniques)	Impact (14 techniques)
Active Scanning (3)	Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation (7)	Abuse Elevation Control Mechanism (6)	Abuse Elevation Control Mechanism (6)	Adversary-in-the-Middle (4)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (4)	Application Layer Protocol (5)	Automated Exfiltration (1)	Account Access Removal
Gather Victim Host Information (4)	Acquire Infrastructure (8)	Drive-by Compromise	Command and Scripting Interpreter (11)	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (3)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction (1)
Gather Victim Identity Information (3)	Compromise Accounts (3)	Exploit Public-Facing Application	Container Administration Command	Boot or Logon Autostart Execution (14)	Account Manipulation (7)	BITS Jobs	Credentials from Password Stores (6)	Browser Information Discovery	Lateral Tool Transfer	Audio Capture	Content Injection	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Gather Victim Network Information (6)	Compromise Infrastructure (8)	External Remote Services	Deploy Container	Boot or Logon Initialization Scripts (5)	Boot or Logon Autostart Execution (14)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Automated Collection	Data Encoding (2)	Exfiltration Over C2 Channel	Data Manipulation (3)
Gather Victim Org Information (4)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Browser Extensions	Boot or Logon Initialization Scripts (5)	Debugger Evasion	Forced Authentication	Cloud Service Dashboard	Remote Services (8)	Browser Session Hijacking	Data Obfuscation (3)	Exfiltration Over Other Network Medium (1)	Defacement (2)
Phishing for Information (4)	Establish Accounts (3)	Phishing (4)	Inter-Process Communication (3)	Compromise Host Software Binary	Create or Modify System Process (5)	Deobfuscate/Decode Files or Information	Forge Web Credentials (2)	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data	Dynamic Resolution (3)	Exfiltration Over Physical Medium (1)	Disk Wipe (2)
Search Closed Sources (2)	Obtain Capabilities (7)	Replication Through Removable Media	Native API	Create Account (3)	Domain or Tenant Policy Modification (2)	Deploy Container	Input Capture (4)	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Storage	Encrypted Channel (2)	Exfiltration Over Web Service (4)	Endpoint Denial of Service (4)
Search Open Technical Databases (5)	Stage Capabilities (6)	Supply Chain Compromise (3)	Scheduled Task/Job (5)	Create or Modify System Process (5)	Escape to Host	Direct Volume Access	Modify Authentication Process (9)	Container and Resource Discovery	Taint Shared Content	Data from Configuration Repository (2)	Fallback Channels	Scheduled Transfer	Financial Theft
Search Open Websites/Domains (3)		Trusted Relationship	Serverless Execution	Event Triggered Execution (17)	Event Triggered Execution (17)	Domain or Tenant Policy Modification (2)	Multi-Factor Authentication Interception	Debugger Evasion	Use Alternate Authentication	Data from Information Repositories (5)	Hide Infrastructure	Transfer Data	Firmware Corruption
Search Victim-Owned Websites		Valid Accounts (4)	Shared Modules	External Remote		Execution Guardrails (2)	Multi-Factor	Device Driver Discovery		Data from Local System	Ingress Tool Transfer		Inhibit System Recovery
			Software Deployment Tools			Exploitation for Defense Evasion		Domain Trust Discovery					Network Denial of Service (2)
						File and Directory Permissions Modification (2)		File and Directory					Resource Hijacking (1)

From another lens

Not a direct application of techniques, but aligns to the framework

Reconnaissance	*high value wallet(s) & infra identified, public info*
Initial Access, Execution	*developer's computer breached*
Credential Access, Privilege Escalation	*gaining backend privileged access to public website*
Defense Evasion ->	*malicious javascript w/specific triggers*
Impact ->	*complex financial theft*

How hard is reconnaissance, to identify valuable crypto wallets and multisig configs?
In this case:

- Publicly visible wallet holdings and transaction history (on Ethereum blockchain)
- Likely publicly visible multisig wallet configurations & transaction history

What about the web3 part?

Technical level

- Smart contracts are called “smart” for a reason
- Signing them is complicated
- Digital “fine print” a.k.a blind signing is easy for humans to miss
  .. also, a 3rd party vendor (web2) attack combined with a web3 attack

Business level

- Systems and processes are complex, involve lots of little tradeoffs
- Designing for secure human computer interaction is hard
- Transaction signers generally aren’t cybersecurity experts
- The systems and processes that failed were probably considered sufficient, at least sometime in the past

* It’s easy to be a Monday morning quarterback

So why does this happen?

First, keep in mind

- Publicly shared hack analysis only tells part of the story
- Don't know how much the companies invested in infosec
  Even with significant investment, ROI can vary widely
- Cyber offense vs. defense are not always equally difficult
- Cyber attacks tend to evolve - the goal line moves
- Managing 3rd party security risks is hard
- Private businesses are left to fend for themselves too much against organized crime and nation state hacking

Why in this case?

.. on the multisig wallet provider side

- A user device and production access was breached
- Production tampering or modification was not detected, or not fast enough

-> common struggles across many industries

.. on the impacted crypto operation

- The cryptography was strong, but humans interacting with it were tricked

-> common struggle across many industries and uses of cryptography

Lots of defense-in-depth controls *could* be creatively built for these specific areas

However, this is only one of many areas to secure

Why, more broadly?

Very personal opinion. A cryptocurrency industry combination of:

- *Overconfidence & Dunning-Kruger effect*
- *Short-lived, volatile, and lucrative business opportunities*
- *Viewing security as a cost more than a selling point*
- *The journey to becoming profitable involves multiple forms of existential risks*

A personal opinion

Strong, creative, innovative, industry-leading information security is expensive

Companies operating with crypto that can absorb a $1billion loss, can afford it

Common myths

Myth: infosec should help with the techy parts like encryption and vulnerabilities, not operational business processes

Myth: smart contract audits cover everything

Myth: apple gear is so secure that corporate device controls are unnecessary

Myth: monitoring and privileged access controls are just for the really big companies

Myth: we don't need to check on patching, it works automatically

Myth: we can't be phished or tricked, we only click the safe links

Myth: the next crypto hack victim will always be someone else

What to do

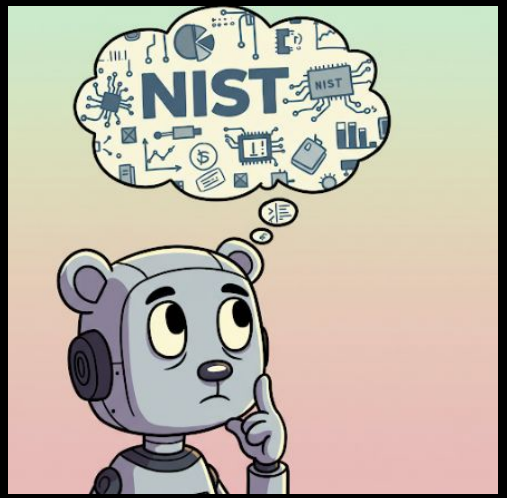
Back to the basics!
Approach strong security as a primary business objective!
Disciplined and comprehensive security!

- NIST CSF, NIST 800-53, MITRE, OWASP, CWE, CCSS, and more
- Assess risks, continuously understand threats and vulnerabilities
- Threat model
- Architect and build protective controls
- Build defense-in-depth
- Monitor
- Build response and recovery capabilities
- Govern and invest in securing assets
- DR, BCP, Asset Inventories
- Audit, Assess, Pen test, Enlist help from experts
- Address insider threats
- .. and much more

NIST Framework examples

E.g. NIST 800-53 covers a ton of controls. These look *very* similar to web3 needs:

- Process isolation and hardware separation
  -> *Crypto hardware wallets*
- Detonation chambers for quickly identifying malicious code
  -> *Crypto transaction simulations*
- Cryptographic mechanisms to detect unauthorized changes to software, firmware, and information
- PKI controls
- .. and more



Topics for another day...

Custodial funds
Backups and failover
Hardware security for signing
Cold signing
Defi exchanges
Smart contract security
CI/CD security
Hardware wallets vs. cold signing
3rd party risks
Secure communications
High integrity transaction instructions
KYC and KYT
Wallet and keys registry
Physical protections
Insider threats
Monitoring and real-time visibility
...

Thanks!

Reach out - https://www.linkedin.com/in/ethan-johnson-9184956

Ethan Johnson

Next Encrypt - Consulting and Advising

Fractional Chief Information Security Officer Services